NETA SCIENTIFIC DISASTER RECOVERY PLAN

Section 1: Introduction

The employees of Neta Scientific HQ all rely heavily on the Information Technology (IT) infrastructure and services to accomplish their work.

As a result of this reliance, IT services are considered a critical component in the daily Operations of Neta Scientific HQ, requiring a Disaster Recovery Plan to assure that these services can be re-established quickly and completely in the event of a disaster.

This IT Disaster Recovery Plan presents the requirements and the steps that will be taken in response to and for the recovery from any disaster affecting IT services at Neta Scientific HQ, with the fundamental goal of allowing basic business functions to resume and continue until such time as all systems can be restored to pre-disaster functionality.

This plan is reviewed and updated annually by IT staff and approved by the VP of Operations.
A copy of this plan is stored in the following areas:

- VP of Operations.
- IT SOPs.

Section 2: Scope

Due to the uncertainty regarding the magnitude of any potential disaster at Neta Scientific HQ, this plan will only address the recovery of systems under the direct control of the Neta Scientific's IT department that are critical for business continuity. This includes the following major areas:

- Servers including Active Directory Services.
- On-premises enterprise applications. (Microsoft GP, SalesPad, ShipTo)
- Desktop equipment.
- Data networks and telecommunications. (Wired and wireless networks, file services, telephony)

There are a number of other servers and services that aren't hosted at Neta Scientific HQ, including systems crucial for daily the activities. The recovery of these systems themselves are beyond the scope of this document and the ability of our internal IT department.

This includes but not limited to the following major services:
- Hosted enterprise applications (Office365, AutoPO, Punchout sites, Company websites)

Section 3: Assumptions

This disaster response and recovery plan is based on the following assumptions:
Once an incident covered by this plan has been declared a disaster, the appropriate priority will be given to the recovery effort and the resources and support required as outlined in the IT
Disaster Recovery Plan will be available.

The safety of Neta Scientific HQ employees and faculty are of primary importance and the safeguard of such will supersede concerns specific to hardware, software and other recovery needs.
Depending on the severity of the disaster, other departments may be required to modify their operations to accommodate any changes in system performance, computer availability and physical location until a full recovery has been completed.
Information Technology will encourage all other departments to have contingency plans and
Business Continuity Plans for their operations, which include operating without IT systems for a period of time.

Section 4: Definitions

Disaster: Any IT incident which is determined to have potential impacts on the business continuity and ongoing operations of Neta Scientific HQ.

Backup/Recovery: Copies of all software and data located on the servers, which are used to return the servers to a state of readiness and operation that existed shortly prior to the incident/disaster.

Catastrophic Disaster: A catastrophic disaster will be characterized by expected downtime of greater than 7 days. Damage to the system hardware, software, and/or operating environment requires total replacement / renovation of all impacted systems.

Desktop Recovery Team: Individuals responsible for the recovery and testing of desktop computers and services in the affected areas at Neta Scientific HQ.

Disaster Recovery Team: The DRT is a team of individuals with the knowledge and training to recover from a disaster.

Equipment Configuration: A database (either soft or hard copy) which documents the configuration information necessary to return any IT hardware (server, network, desktop) to pre-disaster configurations. This includes hardware revisions, operating system revisions, and patch levels.

Incident: Any non-routine event which has the potential of disrupting IT services to Neta Scientific HQ. An incident can be a fire, wind storm, significant hardware failure, flood, virus, Trojan horse, etc.

Major Disaster: A major disaster will be characterized by an expected downtime of more than
48 hours but less than 7 days. A major disaster will normally have extensive damage to system hardware, software, networks, and/or operating environment.

Infrastructure and Web Recovery Team: Individuals responsible for the recovery and testing of infrastructure systems at Neta Scientific including Active Directory, DNS, email, and web services. In the cases where these services are hosted off-premises, this team is responsible for re-establishing connectivity, authentication, and integration of those systems.

Minor Disaster: A minor disaster will be characterized by an expected downtime of no more than 48 hours, and minor damage to hardware, software, and/or operating environment from sources such as fire, water, chemical, sewer or power etc.

Enterprise Applications Recovery Team: For those systems hosted off-premises, such as AutoPO. This team is responsible for re-establishing connectivity, authentication, and integration of those systems.

Routine Incident: A routine incident is an IT situation/failure that is limited in scope and is able to be addressed and resolved by a specific team or individual as part of their normal daily operations and procedures.

Network and Telecommunications Recovery Team: Individuals responsible for the recovery and testing of data and voice networks.

Web Services: All services related to Neta Scientific's Internet and intranet web activities and presence.

Section 5: Teams

5.1 Desktop Recovery Team

The Desktop Recovery Team is composed of personnel within the Information Technology department that support desktop hardware and client applications. The primary function of this working group is the restoration of Neta Scientific HQ desktop systems to usable condition. During the initial recovery effort, the team is not responsible for restoration of any data the user may have on their desktop computer.

Neta Scientific's IT staffs recommends all users store data files on the file servers, which are backed up nightly, to support data recovery. The team should be mobilized in the event that a significant interruption in desktop has resulted from unexpected/unforeseen circumstances and requires recovery efforts in excess of what is experienced on a normal day-to-day basis.

The team lead has the responsibility to keep the Executive Team up to date regarding the nature of the disaster and the steps being taken to address the situation. The coordination of this recovery effort will be accomplished with the other recovery efforts at Neta Scientific HQ.

Team Lead:	Database Administrator
Team Members:	IT Manager
	Assistant IT Manager
	Webmaster

5.2 Enterprise Systems Recovery Team

The Enterprise Systems Recovery Team is composed of personnel within the Information Technology department that support AutoPO, Microsoft GP, SalePad and other enterprise systems. The primary function of this working group is the restoration of all Business applications to the most recent pre-disaster configuration in cases where data or operational loss is significant. In less severe circumstances the team is responsible for restoring the system to functional status as necessitated by any hardware failures, network outages, or other circumstances that could result in diminished system operation or performance.

The team lead has the responsibility to keep the Executive Team up to date regarding the nature of the disaster and the steps being taken to address the situation.

Team Lead:	IT Manager
Team Members:	Assistant IT Manager
	Consultant (Programmer)
	Vendor Support

5.4 Infrastructure and Web Recovery Team

The Infrastructure and Web Recovery Team is composed of personnel within the Information Technology department that support the company's network infrastructure, including Active Directory, DHCP, DNS, email, file servers, network applications, network storage and web services. The primary function of this working group is the restoration of our network infrastructure and servers to their most recent pre-disaster configuration in cases where data and operational loss is significant. In less severe circumstances, the team is responsible for restoring the system to a functional status as necessitated by any hardware failures or other circumstances that could result in diminished operation or performance.

In the case of off-premises services, this team will coordinate restoration of these services with the external vendors or organizations responsible for providing them.

The team lead has the responsibility to keep the Executive Team up to date regarding the nature of the disaster and the steps being taken to address the situation.

Team Lead:	IT Manager
Team Members:	Assistant IT Manager
	Database Administrator
	Webmaster

5.5 Telecommunications, Network, and Internet Services Recovery Team

The Telecommunications, Network, and Internet Services Recovery Team is composed of personnel within the Information Technology department that support the company's voice and data networks including cables, switches, and routers. The primary function of this working group is the restoration of our voice and data networks and Internet services to the most recent pre-disaster configuration in cases where operational loss is significant.

In less severe circumstances, the team is responsible for restoring the voice and data networks and Internet services to a functional status as necessitated by any failures or other circumstances that could result in diminished operation or performance.

The team should be mobilized in the event that any component of the voice or data networks experiences a significant interruption in service that has resulted from unexpected/unforeseen circumstances and requires recovery efforts in excess of what is experienced on a normal day-to-day basis.

The team lead has the responsibility to keep the Executive Team up to date regarding the nature of the disaster and the steps being taken to address the situation.

Team Lead:	IT Manager
Team Members:	Assistant IT Manager
	Database Administrator

5.6 Critical Neta Scientific Contacts

Winfred Sanders	
Garnetta Sanders	
Brandi Toatley	
Eric Toatley	
Dragan Karajovic	

Section 6: Recovery Preparations
A critical requirement for disaster recovery is ensuring that all necessary information is available to assure that hardware, software, and data can be returned to a state as close to "pre-disaster" possible. Specifically, this section addresses the backup and storage practices as well as documentation related to hardware configurations, applications, operating systems, support packages, and operating procedures.

6.1 Data Recovery Information:
Backup/Recovery drive (DISKSTATION) and Acronis software are required to return systems to a state where they contain the information and data that was resident on the system shortly prior to the disaster. System backups are governed by the SOP Backup procedure, located at Neta Scientific HQ. The backup drive locations and retention periods summarized in the table below

Type:	Location:
Daily Backup (disk)	Neta Scientific HQ (DISKSTATION)
Weekly Backup (disk)	Neta Scientific HQ (DISKSTATION) Off-site storage (Eric's/DISKSTATION2)

Neta Scientific does not currently have systems in place to backup and restore information/data located on individual desktop systems throughout HQ. Only the servers located at HQ are backed up; as such, only data resident on these systems will be able to be recovered. In the event that a disaster at HQ which destroys personal computers, the information located on these computers will be extremely difficult or impossible to recover. If recovery is possible, it will require outside vendor involvement and it will be expensive.

The Information Technology department recommends and encourages the use of network drives (on servers) to store all important files. The recovery of data not backed up to a network drive and/or full system backups are not covered under this plan.

6.2 Neta Scientific HQ and Server Recovery Information:
In the event of any disaster which disrupts the operations at Neta Scientific HQ, reestablishing HQ will be the highest priority and a prerequisite for any IT recovery. As such, the Information Technology department is required to have detailed information and records on the configuration of the HQ and all servers and ancillary equipment located at HQ. Detailed information is documented in the IT SOPs. The IT staff is responsible for keeping the hardware inventory up to date.

6.3 Network and Telecommunication Recovery Information:
In the event of any disaster which disrupts the network and/or telecommunications, reestablishing the connectivity and telephony will be a high priority and a prerequisite for any IT recovery. Recovery of these services will be accomplished in parallel or immediately following recovery of the HQ servers. As such, Information Technology is required to have detailed information and records on the configuration of the networking equipment.

Detailed information of switches and routers are documented in the IT SOP documents. The IT staff are responsible for keeping the hardware inventory up to date.

6.4 Application Recovery Information:
Information necessary for the recovery and proper configuration of all application software located on the central servers is critical to assure that applications are recovered in the identical configuration as they existed prior to the disaster. Detailed information on critical central applications will be documented in the IT SOPS. The IT staff is responsible for keeping the software inventory up to date.

6.5 Desktop Equipment Recovery Information:
Information necessary for the recovery and proper configuration of all desktop computers and printers supported by Information Technology Services is critical to assure that client systems can be restored to a configuration equivalent to pre-disaster status. Detailed information on client systems are documented in the IT SOPs. The infrastructure staff is responsible for keeping the hardware inventory up to date.

Section 7: Disaster Recovery Processes and Procedures

7.1 Emergency Response:

The requirement for the usage of the DRP will be dependent on the size and type of the incident.

Examples of situations which will normally result in the involvement of the DRP include:
Severe structural damage to the facility where personal safety is in question, and where analysis must be completed to assure the building is acceptable for access. This would include, but is not limited to, damage from a flood or tornado. Environmentally hazardous situations such as fires, explosions, or possible chemical or biological contamination where the situation must be contained prior to building occupancy. Flooding or other situations which may pose the risk of electrical shock or other life-threatening situations.

Examples of situations which will normally not result in the total involvement of the DRP include:
Major system/hardware failures that do not pose a hazard to personnel or property. Utility outages (electrical, etc.) which are remote to the HQ being affected.

7.3 Disaster Recovery Teams:

The Disaster Recovery Teams are organized to respond to disasters of various types and sizes. Any or all of these teams may be utilized depending on the parameters of the disaster. It is the responsibility of the IT supervisor to determine which Disaster Recover Team/s to mobilize, following the declaration of a disaster and the notification of the Executive Management Team. Each team will utilize their respective procedures, disaster recovery information, technical expertise, and recovery tools to expeditiously and accurately return their systems to operational status. While recovery by multiple teams may be able to occur in parallel, HQ and the network/telecommunications infrastructure will normally be assigned the highest priority, as full operational recovery of most other systems cannot occur until these areas are operational.

7.3.1 Server Recovery Team:

1. Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
2. Assess damage and make recommendations for the recovery of the Domain servers.
3. If the alternate location is required, execute all necessary steps to notify appropriate personnel and secure backup facility.
4. Identify other individuals required to assist in the recovery of the Domain servers.
5. Develop overall recovery plan and schedule, focusing on highest priority servers for specific applications first.
6. Coordinate hardware and software replacements with vendors.
7. Recall backup/recovery files from HQ or Off-site storage, as required to return damaged systems to full performance.

8. Oversee recovery of Domain servers based on established priorities.
9. Coordinate domain server recovery with other recovery efforts at HQ if necessary.
10. Provide scheduled recovery status updates to the Executive Team to ensure full understanding of the situation and the recovery effort.
11. Verify and certify restoration of the Domain server to pre-disaster functionality.

7.3.2 Desktop Recovery Team:

1. Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
2. Assess damage at all areas affected, and make recommendations for recovery.
3. Identify other individuals required to assist in recovery of desktop services.
4. Develop overall recovery plan and schedule, focusing on highest priority areas of the HQ infrastructure/desktop services first.
5. Coordinate hardware and software replacement with vendors.
6. Oversee recovery of desktop computing services (workstations, printers, etc.) based on established priorities.
7. Coordinate recovery with other recovery efforts at HQ.
8. Provide scheduled recovery status updates to the Executive Team to ensure full understanding of the situation and the recovery effort.
9. Verify and certify restoration of the desktops to pre-disaster functionality.

7.3.3 Enterprise Systems Recovery Team:

1. Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
2. Assess damage and make recommendations for the recovery of AutoPO, Microsoft GP, SalesPad and all other enterprise systems.
3. Identify other individuals required to assist in recovery of these applications.
4. Restore degraded system functionality at backup site if necessary and inform user community of the restrictions on usage and/or availability.
5. Coordinate software support/replacement with vendor as required.
6. Coordinate the Enterprise System Recovery as the HIGHEST priority.

7. Execute the plan to restore the Enterprise System services to full functionality.
8. Provide scheduled recovery status updates to the Executive Team to ensure full understanding of the situation and the recovery effort.
9. Verify and certify restoration of the Enterprise Systems services to pre-disaster functionality.

7.3.4 Infrastructure and Web Recovery Team:

1. Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
2. Assess damage and make recommendations for recovery.
3. Identify other individuals required to assist in recovery of services.
4. Develop overall recovery plan and schedule, focusing on highest priority areas of Neta Scientific HQ infrastructure first.
5. Coordinate hardware and software replacement with vendors.
6. Oversee recovery of messaging, telecommunications and network services based on established priorities.
7. Coordinate messaging, network and web systems recovery with other recovery effort at HQ.
8. Provide scheduled recovery status updates to the Executive Team to ensure full understanding of the situation and the recovery effort.
9. Verify and certify restoration of the Messaging, Network and web infrastructure to pre-disaster functionality.

7.3.5 Telecommunications, Network, and Internet Services Recovery Team:

1. Take appropriate steps to safeguard personnel and minimize damage to any related equipment and/or software.
2. Assess damage and make recommendations for recovery.
3. Identify other individuals required to assist in recovery of these services.
4. Develop overall recovery plan and schedule, focusing on highest priority areas of HQ infrastructure first.
5. Coordinate hardware/software replacement with vendors as required.
6. Oversee recovery of voice network services based on established priorities.
7. Coordinate the voice network recovery with other recovery efforts.

8. Provide scheduled recovery status updates to the Executive Team to ensure full understanding of the situation and the recovery effort.

9. Verify and certify restoration of the phones, internet and network services to pre-disaster functionality.

7.4 General System/Application Recovery Procedures/Outline:
The following steps are guidelines to be followed for the overall restoration of systems located at Neta Scientific HQ. While each recovery team has specific duties and responsibilities as outlined in Section 7.3, coordination between the various teams is required to restore operations to the users. While the coordination and extent of personnel involved will depend on the type and severity of the disaster, the following steps may be required:

It is implied in the procedure/outline below that steps are simply provided as a guideline. The magnitude and type of disaster, and the number of systems affected will require that certain steps be augmented (at the discretion of the Executive Team), and that other steps will not be applicable to the situation at hand.

1. Determine extent of damage and make determination as to the following:
    a. Neta Scientific HQ operational/recoverable?
        i. YES: Remain at HQ and initiate recovery accordingly.
        ii. NO: Contact Executive Team and take necessary steps to ready the server room for relocation.
    b. Determine extent of applications affected
        i. AutoPO, Microsoft GP, SalesPad and/or other Enterprise Applications
        ii. Authentication (Active Directory and VPN)
        iii. Web Services (.com, .info, etc…)

    c. Determine extent of desktop/client systems affected throughout HQ.

2. Secure facility as necessary to prevent personnel injury and further damage to IT systems.
    a. Shutdown any active components.

    b. Physically secure facilities (Server room, communication closets, etc.) as necessary to prevent unauthorized access.

3. Retrieve most recent on-site or off-site back-up media. Prepare back-up media for restoration on the HQ servers as determined during the initial assessment.

4. Verify operational ability of all equipment on-site in the affected area (servers, network equipment, ancillary equipment, etc.). If equipment is not operational, initiate actions to repair or replace as needed.

5. Test systems, and communication equipment as required to validate physical operation and performance.
    a. Server testing
    b. Network testing
    c. Desktop/Client testing

6. Upon restoration of the datacenter and servers to operational state:
    a. Restore systems using virtualized images
    b. If necessary, load operating system and test/validate
    c. If necessary, load application software and test/validate
    d. If necessary, load data and verify integrity

7. Verify overall performance of specific system(s) and report readiness to the Management Team, and user community.